Purpose: To ensure that the North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices adhere to a change management process.

STANDARD

1.0 Background

The Divisions and Offices management, with assistance from the Division Information Security Official (ISO), shall ensure that a change management process is developed and planned to ensure information resources are updated appropriately. The Divisions and Offices must establish their own Change Management policies, procedures, standards and guidelines.

2.0 Developing and Planning a Change Management Process

All Divisions and Offices management must ensure that a change management process is established by securing and safeguarding the following change management criteria:

- Define and develop Division and Office policies and procedures that will govern information resource changes
- Define the location (e.g., on-site or off-site) of the information resources that have potential for change
- Define the business owners of the information resources
- Define the proper workforce member's role and responsibility for change implementations
- Define the warning notices that will be relayed to affected DHHS workforce members before, during, or after a change
- Define a contact list to include all the workforce members that must be notified before, during, or after a change
- Define a list of authorized Division and Office management that must be responsible for initiating and/or approving information resource changes

3.0 Creating a Change Management Log

The Divisions and Offices are to create and maintain a change management log of any scheduled and/or emergency information resource changes for auditing purposes. The change management log must be created, maintained, and safeguarded, and must include the following:

- The date and time of the initial change request

- The change request number
- The authorizing manager contact information
- The location of where the change is being performed
- The description of the reason for the change (e.g., software, hardware, etc.)
- The priority categorization of the change and associated timeframe that must correspond with the priority categorization
- The workforce members assigned to make the change
- The processes or steps needed and/or accomplished to complete the change
- The test notes associated with the change and the workforce members who performed the test
- The date the change was completed
- The rollback plans should the implementation not be successful

4.0 Information Resources Owned by Third-Party Vendors

The Divisions and Offices must have assigned workforce members to create a change management log for the changes to information resources that are owned by third-party vendors. The change management log must be created, maintained and safeguarded. The change management log for those information resources that are owned by third-party vendors must at a minimum include the following:

- The date and time the change was implemented
- The departments, workforce members, and/or assets affected by the change
- Contact information for the workforce members that implemented the change
- The description of the change
- The status (e.g., success, failure, etc.) of the change

5.0 Testing Changes

Where appropriate, and prior to implementing any scheduled changes, Divisions and Offices must have assigned workforce members test the changes only. The assigned DHHS workforce members must ensure that test results are recorded and safeguarded in the change management log described above. Test results must be presented when the change requests are submitted to the Division or Office management.

6.0 Change Request Form

The responsibility of creating and documenting a change request form must be determined by the Divisions and Offices management. A change request form must be submitted to the Divisions and Offices management for all changes categorized. The change request form must be approved by the Division or Office management prior to implementing the change. The following change request criteria must be adhered to:

- Upon receiving the change request form, the Division or Office management must determine and record a cost benefit analysis associated with implementing the change request. The cost benefit analysis must be done prior to the change being implemented into the production environment.

Section II: **NC DHHS Security Standards**   **Page 2 of 4**
Title: **Information Security Change Management Standard**
Current Effective Date: **June 30, 2008**

- The Divisions and Offices management must ensure that the requested change, if approved, is performed at a pre-determined authorized time. The Divisions and Offices management may approve a scheduled change to be performed on an as-needed basis.
- The change request form shall include the testing results, if testing was deemed necessary.
- If the change is *approved,* the Division or Office management signature(s) must be recorded on the change request form. The Division or Office BCP Coordinator must be notified to ensure that all Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) documents are updated appropriately. Once approved, the DHHS Divisions and Offices must follow Section 8.0: Executing a Change.
- If the change is *not approved,* then the Divisions and Offices management must sign-off that the change was not approved with documented reasons explaining why the change will not be implemented. The Divisions and Offices management must immediately notify appropriate workforce members that the change request has been denied.

The Divisions and Offices management shall ensure that the change request form is secured and safeguarded once an approval decision is made.

7.0 Emergency Changes

Upon determining that an emergency change must be implemented, the proper Division or Office management must be notified. Once notified, the Division and Office management must determine an approved implementation time for the change. Once the time has been determined, assigned DHHS workforce members must execute the emergency change. If the change implementation was successful, the Division or Office management must notify the DHHS BCP Coordinator to ensure proper BCP/COOP documentation is updated appropriately. If the change implementation was not successful then the Division and Office management must determine the next course of action. All assigned DHHS workforce members involved will ensure that proper security information is recorded, secured, and safeguarded in the change management log, as it relates to the emergency change.

8.0 Executing a Change

Assigned DHHS workforce members responsible for executing an information resource change shall, at a minimum, perform the following:

- Ensure proper support is available and prepared to assist the appropriate DHHS workforce members that will be affected by the change.
- Determine if any information resource availability will be affected, while the change is being implemented.
- Execute the change by following the necessary steps. The necessary steps of execution must be approved by the Division or Office management and must include when the change will be implemented.
- Verify that the implemented change was *successful* or *unsuccessful* to ensure that the information resource is operable.

Section II: NC DHHS Security Standards
Title: Information Security Change Management Standard
Current Effective Date: June 30, 2008

Page 3 of 4

- Notify proper Division or Office management to *whether* or *not* the changes were implemented successfully.
- Provide instruction to the DHHS workforce members who are affected by the change.

Once the change has been successfully implemented, the assigned DHHS workforce members must ensure that all information in the change management log is updated as appropriate. The completed change management log must then be secured and safeguarded by an appropriate DHHS workforce member. The change management log must be stored in a secure location in order to guard against any type of tampering or malice. All audit logs must be secured and safeguarded in accordance with the General Schedule for State Agency Record – Information Technology Records issued by the NC Department of Cultural Resources – Government Records Branch.

References:

- NC Department of Cultural Resources
  - o Government Records Branch
    - General Schedule for State Agency Record – Information Technology Records

- NC Statewide Information Security Manual, Version No. 1
  - o Chapter 3 – Processing Information and Documents, Section 02: System Operation and Administration
    - Standard 030209 – Scheduling System Operations
    - Standard 030210 – Scheduling Changes to Routine System Operations
  - o Chapter 3 – Processing Information and Documents, Section 05: Data Management
    - Standard 030504 – Permitting Emergency Data Amendment
  - o Chapter 8 – Developing and Maintaining In-House Software, Section 01: Controlling Software Code
    - Standard 080103 – Controlling Software Code During Software Development